

# Troubleshoot Telepresence Endpoint Added to TMS Changing to Behind the Firewall Status Automatically

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Component Used](#)

[Problem](#)

[Troubleshoot](#)

[Solution](#)

## Introduction

This document describes how to isolate the IP address that sends packets to the Telepresence Management Server (TMS) on behalf of the endpoint, causing the issue. When any managed device is added to TMS, its status shows Reachable on LAN by default for sometime however after sometime the status might change to Behind the Firewall. This generally happens when packets received from device have source IP address different from the system IP address that is received from device's xstatus by the TMS.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Telepresence Endpoint running TC (Telepresence Codec) software or MXP
- TMS

### Component Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Problem

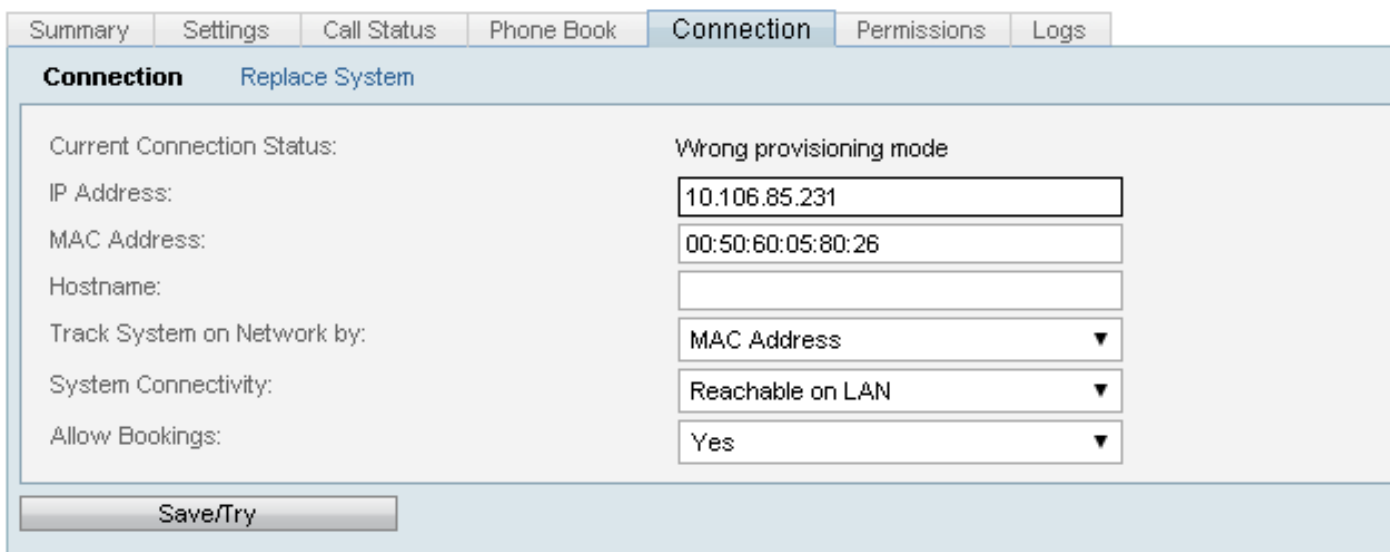
Endpoints managed by the TMS change from Reachable on LAN status to Behind the firewall status automatically, causing the TMS to stop the management of the device. It is considered that

in order to troubleshoot, you must have HTTP communication that is allowed in the network between the managed device and the TMS.

## Troubleshoot

In order to verify a packet capture from the TMS is required :

1. Connect to TMS server via Remote Desktop Protocol (RDP).
2. Ensure that TMS and endpoint have HTTP communication enabled and that HTTPS is disabled.
3. Install/Run Wireshark and Select default network interface.
4. Do not apply any filter and start the capture.
5. Navigate to Connection tab of the endpoint with which you are facing issue, Click **Save/Try** button as shown in this image.



The screenshot shows the 'Connection' tab in a management interface. The 'Current Connection Status' is 'Wrong provisioning mode'. The configuration fields are as follows:

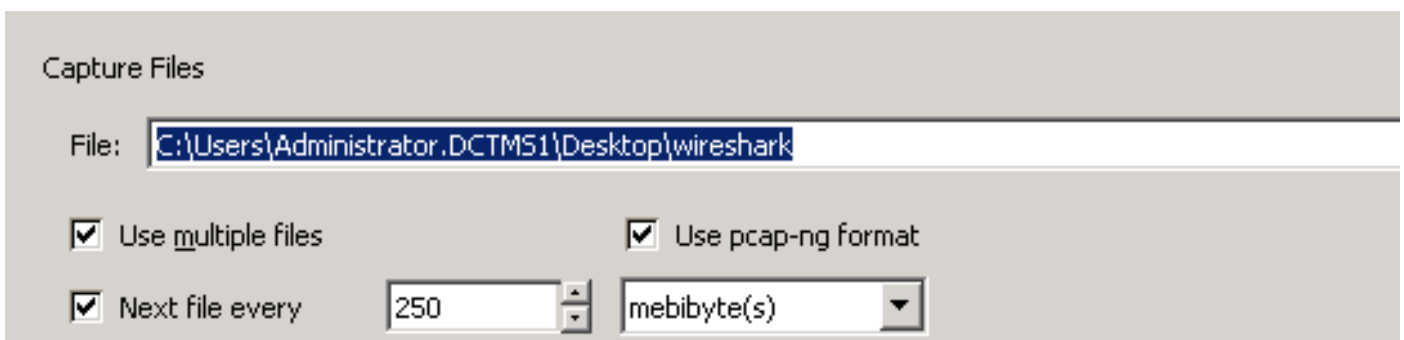
Current Connection Status:	Wrong provisioning mode
IP Address:	10.106.85.231
MAC Address:	00:50:60:05:80:26
Hostname:	
Track System on Network by:	MAC Address ▼
System Connectivity:	Reachable on LAN ▼
Allow Bookings:	Yes ▼

A 'Save/Try' button is located at the bottom of the configuration area.

6. When endpoint falls back to behind firewall, stop wireshark capture.

**Note:** Sometimes the issue might take longer than is expected. To re-create hence while starting the Wireshark capture ensure to save in multiple file.

7. Go to **Capture File** option and select the **Use multiple files** check box.



The screenshot shows the 'Capture Files' configuration dialog. The 'File' field contains the path: `C:\Users\Administrator.DCTMS1\Desktop\wireshark`. The following options are checked:

- Use multiple files
- Use pcap-ng format

The 'Next file every' field is set to 250, and the unit is set to 'mebibyte(s)'.

### Open Wireshark

- Apply filter such as `xml.cdata == IP_ADDRESS_OF_DEVICE`
- After applying this filter you might see that response will change from actual device ip address

to some different ip address.

As shown in this image, the actual IP address of device is x.x.x.174; however later this IP changes to x.x.x.145

The image shows a Wireshark packet capture window with a filter set to 'xml.cdata==157.128.201.145'. The table below represents the data shown in the packet list pane:

No.	Time	Source	Destination	Protocol	Length	Info
5001	45.112269	174	10.61.71.4	HTTP/*	1042	POST /tms/public/external/management/systemmanagementservice.asr
5302	45.759734	174	10.61.71.4	HTTP/*	104	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
5410	45.938035	174	10.61.71.4	HTTP/*	446	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
8025	50.725647	174	10.61.71.4	HTTP/*	1038	POST /tms/public/external/management/systemmanagementservice.asr
8419	51.353143	174	10.61.71.4	HTTP/*	148	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
9205	52.664311	174	10.61.71.4	HTTP/*	914	POST /tms/public/feedback/postdocument.aspx HTTP/1.1
12154	75.116110	145	10.61.71.4	HTTP/*	1364	HTTP/1.1 200 OK
12221	75.754949	145	10.61.71.4	HTTP/*	155	HTTP/1.1 200 OK
12334	76.496791	145	10.61.71.4	HTTP/*	1364	HTTP/1.1 200 OK

Due to change of this IP address, the TMS verifies that the device IP address sent in xstatus is not the same as the IP address in IP header and hence it changes the device to Behind the firewall status.

## Solution

To solve this issue you need to ensure that there is no device in the network between the Endpoint and TMS that is changing source IP address in IP header, hence causing the Source IP in the IP header to be different from the actual IP of the endpoint.